UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P O Box 1450
Alexandria, Virginia 22313-1450
www uspto gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/771,967	01/30/2001	Mehdi-Laurent Akkar	AKKAR	2638

1444 7590 04/28/2009
BROWDY AND NEIMARK, P.L.L.C.
624 NINTH STREET, NW
SUITE 300
WASHINGTON, DC 20001-5303

EXAMINER	
DAVIS, ZACHARY A	

ART UNIT	PAPER NUMBER
2437	

MAIL DATE	DELIVERY MODE
04/28/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	**Application No.** 09/771,967	**Applicant(s)** AKKAR ET AL.	
	Examiner Zachary A. Davis	**Art Unit** 2437	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *19 February 2009*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *15-19,22-24 and 27-34* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *15-19,22-24 and 27-34* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114 was filed in this application after appeal to the Board of Patent Appeals and Interferences, but prior to a decision on the appeal. Since this application is eligible for continued examination under 37 CFR 1.114 and the fee set forth in 37 CFR 1.17(e) has been timely paid, the appeal has been withdrawn pursuant to 37 CFR 1.114 and prosecution in this application has been reopened pursuant to 37 CFR 1.114. Applicant's submission filed on 19 February 2009 has been entered.

2. By the above submission, Claims 15-19, 22-24, 27-29, and 31-34 have been amended. Claims 20 and 21 have been canceled. No new claims have been added. Claims 15-19, 22-24, and 27-34 are currently pending in the present application.

Response to Amendment

3. It is noted that the present response does not fully comply with the provisions of 37 CFR 1.121(c). In particular, the amendments to the claims include text that has not been marked correctly to indicate the changes made relative to the immediate prior version of the claims as required by 37 CFR 1.121(c)(2). At least Claim 16 includes text, marked as deleted, that was not present in the previous version of the claim.

Further, at least Claim 34 includes text that was not present in the previous version of the claim but has not been marked as added by underlining. Additionally, Claim 34 includes text that is both underlined and struck through, which is generally unclear, although it does appear from context that all of this text is intended to be deleted. However, because the present response appears to be a *bona fide* attempt to advance the prosecution of the present application, the response has been treated as though it were fully in compliance with the requirements of 37 CFR 1.121.

Response to Arguments

4. Applicant's arguments filed 19 February 2009 have been fully considered but they are not persuasive.

Regarding the rejection of Claims 15-24, and 27-34 under 35 U.S.C. 103(a) as unpatentable over applicant admitted prior art in view of Chow et al, US Patent 6594761, and Kocher et al, US Patent 6278783, Applicant generally argues that the features of independent Claim 34 are not taught or suggested by the cited prior art (page 11 of the present response).

In response to applicant's argument that Chow is nonanalogous art (page 12 of the present response), it has been held that a prior art reference must either be in the field of applicant's endeavor or, if not, then be reasonably pertinent to the particular problem with which the applicant was concerned, in order to be relied upon as a basis for rejection of the claimed invention. See *In re Oetiker*, 977 F.2d 1443, 24

USPQ2d 1443 (Fed. Cir. 1992). In this case, Chow is at least reasonably pertinent to the particular problem with which Applicant was concerned. As Applicant notes, Chow is directed to tamper resistance techniques (see page 12 of the present response, citing Chow, column 1, lines 57-67). Applicant further asserts that the claimed method "relates to a system in which a program is not accessible from outside of the microcircuit entity, and therefore cannot be modified" (page 12 of the present response); however, the Examiner submits that what Applicant has described is the very definition of tamper resistance. If a program cannot be modified because it is not accessible, then the program is thus tamper resistant. It is also noted that the preamble of independent Claim 34 recites an intended use of the claim "to resist a DPA [differential power analysis] attack against the microcircuit card"; this also is clearly an indication of tamper resistance. Therefore, since both the present invention and Chow are directed to techniques for tamper resistance, Chow is at the very least reasonably pertinent to the problem with which Applicant is concerned. See also MPEP §§ 2141and 2141.01(a).

In response to applicant's arguments against the references individually, one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.,* 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986). More specifically, Applicant separately argues that the disclosure of Chow does not teach identifying a selected chain of operations as now recited in amended independent Claim 34, but teaches that either an operation or its complement is performed (pages 12-13 of the present response, citing Chow, column 18, lines 65-66), and also separately argues that Kocher discloses mixing random state information but does not disclose randomly choosing which group of operations to execute (pages 13-14 of the present response, citing Kocher, column 6, lines 39-63 and column 2, lines 17-18). However, Applicant does not provide any evidence or explanation as to why the combination as a whole does not suggest the claimed invention. The Examiner submits that the combination of the admitted prior art method of mutual authentication of a server and microcircuit card (page 2, lines 3-11 of the present specification) with the discussion of tamper-proofing by determining whether to perform an operation or its complement in Chow (see Chow, column 18, line 50-column 19, line 13, as previously cited) and the determination of which operations to carry out by random decision as taught by Kocher (see Kocher, column 1, line 66-column 2, line 24; column 9, lines 1-13) when considered as a whole suggest the claimed element of randomly selecting which group of operations to execute, where the groups can include operations or their complements.

Regarding the rejection of Claims 22 and 31, Applicant argues that "Kocher does not disclose incrementing a counter when a random parameter before each operation is selected"; this argument is generally unclear grammatically and the Examiner therefore fails to appreciate this argument. The Examiner notes that Kocher does disclose incrementing various counters (the failure counter is incremented before an operation occurs, see column 9, lines 25-27; also, the round counter is initialized and incremented for each round of operations, see column 10, lines 13-45, and column 11, lines 41-45;

further, the loop counter is initialized and incremented within each round of operations, see column 10, line 39-column 11, line 26).

Regarding the rejection of Claims 23 and 32, Applicant argues that the cited portion of Kocher does not disclose transmitting, with each executed operation, information to be used to determine whether the result should be output in complemented or uncomplemented state (see page 16 of the present response). However, the Examiner respectfully disagrees and submits that the cited prior art does disclose the claim limitations as amended. Specifically, the Examiner submits that, in combination, the disclosures in Kocher that new operations are determined based on a random parameter and that intermediate responses are transmitted (Kocher, column 9, lines 7-13, 30-48, and 62-64; column 2, lines 17-19, as previously cited) and in Chow that information can be included with each operation that includes, *inter alia*, inversions of the output so that the output can be properly determined or verified (Chow, column 19, lines 22-34) at least suggest the claim limitation that information to be used during the step of outputting is transmitted with each operation.

Therefore, for the reasons detailed above, the Examiner maintains the rejection as set forth below.

Claim Objections

5. Claim 33 is objected to because of the following informalities:

Claim 33 recites "randomly selecting a next operation of the of the first chain of operations or the second chain of operations". It appears that one of the instances of the phrase "of the" should be deleted.

Appropriate correction is required.

Claim Rejections - 35 USC § 112

6. The rejection of Claims 20 and 21 under 35 U.S.C. 112, second paragraph, is moot in light of the cancellation of those claims. The rejection of Claims 15-19, 22-24, and 27-34 under 35 U.S.C. 112, second paragraph, as indefinite is NOT withdrawn. Although the amendments to the claims have corrected some of the issues of indefiniteness, the amendments have raised new issues of indefiniteness as detailed below.

7. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

8. Claims 15-19, 22-24, and 27-34 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 34 recites the limitations "storing a first chain of operations in both the server entity and the microcircuit card" in lines 5-6 and "storing, at the microcircuit card, a second chain of operations" in line 8. It is unclear how operations themselves could be stored, as opposed to, for example, instructions or logic for performing those operations. The claim further recites “said first chain of operations forming a data encryption standard” in lines 6-7. This is generally unclear; similar to a previous version of the claim, it is not clear how the chain of operations themselves form a standard or if there is a particular standard being referred to herein. The claim also recites “said second chain of operations comprising a succession of operations each corresponding to a complement of one of said operations in the first chain of operations”. The use of the phrase “one of said operations” is unclear because the extent to which this phrase limits which operation is referred to is too broad, and it is not clear whether the succession of operations has a one-to-one correspondence with the first chain or if operations can be repeated or reordered, for example.

Claim 34 further recites “identifying, in the microcircuit card, a selected chain of operations, said step of identifying comprising randomly choosing one of the following groups as said selected chain: 1) all of the operations in said first chain of operations; 2) all of the operations in said first chain of operations; or 3) a plurality of operations comprising a random selection of at least one of the operations in said first chain of operations and at least one of the operations in said second chain of operations” in lines 32-37 of the claim (page 8 of the present response). First, it is not clear what the difference is between groups 1) and 2) because they both recite all of the operations in the first chain; it appears that one of these may have been intended to refer to the second chain of operations, and it has been assumed for purposes of interpreting the prior art that group 2) was intended to do so. Further, the description of group 3) is somewhat unclear, since it is not clear which operations from the first and second chains of operations are required to be included in the third group. In particular, with respect to the later steps of executing the identified chain on the message and comparing that resultant message to the server result determined previously (see lines 38-39, 43-44, and 47-50 of the claim), it is not clear that the resultant message would even be possible to be identical to the server result if the third group was selected unless further requirements were placed on the third group.

Claim 16 recites the limitation “operations of said first chain of operations preceding said operation of bit permutation”. It is not clear which operations of the first chain, if any, clearly precede or follow any operation of permutation.

Similarly, Claim 19 recites the limitation “operations of said second chain of operations preceding said operation of transfer”. It is not clear which operations of the second chain, if any, clearly precede or follow any operation of transfer.

Claim 22 recites the limitation “the step of outputting as the resultant message is decided depending on a state of the complementation counter”. This is generally unclear, with particular reference to the phrase “the step of outputting… is decided”. It is not clear how one is to decide a step of outputting, or what decision that would clearly encompass.

Claims 23 and 32 each recite the limitation “transmitting, with each executed operation, information to be used during the step of outputting”. However, it is unclear where this information is to be transmitted to or from, which renders the claims indefinite.

Claims 27 and 28 each recite the limitation “the step of storing, at the microcircuit card, a second chain of operations comprises complementing each operation in the first chain of operations”. First, as noted above with respect to Claim 34, it is unclear how operations themselves could be stored, as opposed to, for example, instructions or logic for performing those operations. Further, it is not clear how an operation itself could be complemented while being stored, and the specification does not provide any further illumination in that regard.

Claim 29 recites the limitation “the step of having the microcircuit card determine the second chain of operations”. There is insufficient antecedent basis for this limitation in the claims, although it appears that it may be intended to refer to the step of identifying a selected chain as recited in Claim 34.

Claims 31-33 each recite the limitation “the step of randomly selecting at least one of the operations in the first chain of operations and at least one of the operations in the second chain of operations”. There does not appear to be sufficient antecedent basis for this limitation, as there is no step of randomly selecting previously recited in the claims; however, it appears that this may be intended to refer to the random selection of operations referred to in group 3) of the groups from which the selected chain of operations is to be chosen (see Claim 34, lines 35-37).

Claim 31 further recites the limitation “the step of outputting as the resultant message is decided depending on a state of the complementation counter”. This is generally unclear, with particular reference to the phrase “the step of outputting… is decided". It is not clear how one is to decide a step of outputting, or what decision that would clearly encompass.

Claim 33 further recites the limitation "the step of randomly selecting a next operation". There is insufficient antecedent basis for this limitation in the claims.

Claims not specifically referred to above are rejected due to their dependence on a rejected base claim.

Claim Rejections - 35 USC § 103

9. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

10. Claims 15-19, 22-24, and 27-34 are rejected under 35 U.S.C. 103(a) as being unpatentable over applicant admitted prior art in view of Chow et al, US Patent 6594761, and Kocher et al, US Patent 6278783.

In reference to Claim 34, Applicant admits as prior art a method including storing a first chain of operations that performs DES encryption, exchanging a message between a server entity and a microcircuit card, the server entity applying a first chain of operations to the message to obtain a server result, the microcircuit card applying a second chain of operations to the message to obtain a resultant message, comparing the resultant message to the server result, and the server and card mutually authenticating when the server result and resultant message are identical (see page 2, lines 3-11, of Applicant's specification). However, Applicant's admitted prior art does not explicitly disclose determining the second chain of operations as explicitly derived from the first chain, nor that the determination is made by randomly choosing a group of operations that include some combination of operations of first and second chains of operations in either a complemented or uncomplemented state.

Chow discloses a tamper-proof encoding method that can be used with encryption protocols (see the description of application of the method to DES, starting at column 20, line 28). Chow further discloses that the encoding method includes determining whether to perform an operation or its complement (column 18, line 50-column 19, line 13). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to further modify the prior art method by performing operations in either a normal or complemented state, in order to increase the tamper-resistance and obscurity of computer code (see Chow, column 4, lines 3-9). However, Chow does not explicitly disclose determining whether to perform the operation or its complement based on a random determination.

Kocher discloses a cryptographic protocol in which a chain of operations is carried out (Figures 1 and 2; column 1, line 66-column 2, line 24) and in which operations in the chain can be chosen depending on a random decision (column 9, lines 1-13). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method, described in Applicant's admitted prior art and modified by Chow, by including a random determination of whether to perform an operation or its complement, in order to increase the security of a system (see Kocher, column 1, line 66-column 2, line 9).

In reference to Claims 15-18, Kocher further discloses that XOR operations, permutation operations, indexed access to a table, and operations that are stable with respect to XOR can be used as operations in the chain (column 2, line 44-column 3, line 9, especially column 2, lines 44-45). Chow also discloses permutations and indexed access to a table (column 18, lines 43-49; column 19, lines 52-61; column 20, lines 48-53).

In reference to Claim 19, Kocher further discloses that operations that transfer data between memory locations may be performed (column 8, lines 45-57).

In reference to Claims 20 and 21, Chow further discloses that a decision whether to perform an operation or its complement is made for each operation (column 18, line 65-column 19, line 13).

In reference to Claims 22 and 31, Kocher and Chow further disclose that new operations are determined based on a random parameter (Kocher, column 9, lines 7-13, 30-48, and 62-64, where Chow discloses determining whether to perform an operation or its complement, column 18, line 50-column 19, line 13) and a counter is updated (Kocher, column 9, lines 25-27; column 10, lines 13-column 11, line 26; column 11, lines 41-45).

In reference to Claims 23 and 32, Kocher and Chow further disclose that new operations are determined based on a random parameter (Kocher, column 9, lines 7-13, 30-48, and 62-64, where Chow discloses determining whether to perform an operation or its complement, column 18, line 50-column 19, line 13) and intermediate responses are transmitted (see Kocher, column 2, lines 17-19), and Chow further discloses transmitting information with each executed operation (Chow, column 19, lines 22-34).

In reference to Claims 24 and 33, Kocher further discloses comparing a counter against a threshold value and altering operation based on the comparison (column 9, lines 25-30; see also column 7, lines 21-29).

In reference to Claim 27, Kocher further discloses performing operations byte by byte (see column 5, lines 20-27).

In reference to Claim 28, Kocher further discloses performing operations bit by bit (see column 2, line 45; also column 10, lines 51-60). Chow also discloses bit by bit operation (column 18, lines 65-66).

In reference to Claims 29 and 30, Kocher further discloses that the order of execution of operations can be permuted randomly (column 10, lines 51-55).

Conclusion

11. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a. Jaffe et al, US Patent 6510518, discloses a system used in smartcards and cryptosystems in which a difference between the numbers of complemented operations and uncomplemented operations is minimized.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Zachary A. Davis whose telephone number is (571)272-3870. The examiner can normally be reached on weekdays 8:30-6:00, alternate Fridays off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Zachary A Davis/
Examiner, Art Unit 2437